John A. Yanchunis (Pro Hac Vice to be filed)
Ryan J. McGee (Pro Hac Vice to be filed)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jyanchunis@ForThePeople.com
rmcgee@ForThePeople.com

Clayeo C. Arnold, California SBN 65070
Joshua H. Watson, California SBN 238058
CLAYEO C. ARNOLD, A
PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, California 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
carnold@justice4you.com
jwatson@justice4you.com

Attorneys for Plaintiffs and the Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MICHAEL FORD and RUDOLPH DUBROVSZKY, individually and on behalf of all others similarly situated,

Plaintiff,

v.

24/7, INC., a California Corporation, BEST BUY CO., INC., a Minnesota corporation, and DELTA AIRLINES, INC., a Delaware corporation,

Defendants.

CASE NO.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs, Michael Ford ("Ford" or the "Best Buy Plaintiff") and Rudolph Dubrovszky ("Dubrovszky" or the "Delta Plaintiff"), on behalf of themselves and all others similarly situated, file this Class Action Complaint against Defendants, 24/7, Inc. ("24/7"), Best Buy Co., Inc. ("Best Buy"), and Delta Airlines, Inc. ("Delta") (collectively "Defendants"), and based upon personal knowledge with respect to themselves and on information and belief derived therefrom, among other things, investigation of counsel and review of public documents as to all other matters, allege as follows:

SUMMARY OF THE CASE

1. Plaintiffs bring this class action against Defendants for their failure to secure and safeguard customers' payment card data ("PCD") and other personally identifiable information ("PII") that Defendants collected during customer service support contact with Best Buy and Delta , and for failing to provide timely, accurate, and adequate notice to Plaintiffs and the Class and Subclass members that their PCD and PII (hereinafter, collectively, "Customer Data") had been compromised and stolen.

2. 24/7 is a customer experience software and services company headquartered in San Jose, California, with approximately 12,000 employees. 24/7 offers sales and service-oriented software, as well as voice and chat agent services, for sales and support. Best Buy and Delta have used 24/7 for such services since at least, and likely well before, September 27, 2017—the purported beginning of the data breach described herein.

3. Best Buy is a retail company with over 1,000 stores throughout the United States providing technology products, services, and solutions. Best Buy offers "expert service" more than 1.5 billion times every year to consumers, small business owners, and educators who visit and patronize Best Buy stores. Best Buy also provides the "Geek Squad" service to further facilitate its goal of providing technology products, services, and solutions. Best Buy markets and makes these products and services through various distribution channels including, *inter alia*, its website and over the phone.

4. Delta provides air transportation for passengers in the United States and abroad. Delta offers its services through a system of hubs from Atlanta, Boston, Detroit,

Los Angeles, Minneapolis-St. Paul, New York, Salt Lake City, Seattle, and a number of international gateways. Delta sells tickets through various distribution channels including, *inter alia*, its website, mobile application, and over the phone.

5. In the last few years, retailers such as Target, Home Depot, Neiman Marcus, and Brooks Brothers have experienced streams of attacks on their data security. Implementing measures to prevent those attacks, as well as quickly identifying them, is a normal, expected part of the business—except in Defendants' case.

6. On April 4, 2018, Delta acknowledged that customers using Delta's online chat services, which were outsourced to 24/7, were subject to a data breach. In its statement, Delta stated its customers who used its customer support services during September and October of 2017 were potential victims of a breach in which their Customer Data was "exposed" and compromised (the "Data Breach").[1] The Data Breach included payment information and other Customer Data.[2]

7. On April 5, 2018, Best Buy acknowledged that customers who used Best Buy's outsourced chat services for customer support were similarly potential victims of the Data Breach and their Customer Data was stolen. Best Buy only acknowledged the Data Breach, however, after 24/7 informed Best Buy of the Data Breach, and after other companies—namely Delta and Sears—acknowledged the same Data Breach.[3]

8. This private Customer Data was compromised due to Best Buy's and Delta's, as well as their agent 24/7's, acts and omissions and their failure to properly protect the Customer Data.

9. Defendants could have prevented this Data Breach. Data breaches in the last few years have been the result of infiltration of computer systems in which Customer Data is exchanged. While many retailers, restaurant chains, and other companies using such

[1] Delta, *Updated: Statement on [24]7.ai cyber incident*, https://news.delta.com/updated-statement-247ai-cyber-incident (last visited April 30, 2018).

[2] *Id.*; AP, *Delta says customers' payment info breached in cyberattack*, https://nypost.com/2018/04/04/delta-says-customers-payment-info-breached-in-cyberattack/ (last visited April 30, 2018).

[3] Brian Heater, *Best Buy Customer Info may have been Exposed in Data Breach*, TechCrunch, https://techcrunch.com/2018/04/06/best-buy-customer-info-may-have-been-exposed-in-data-breach/ (last visited April 30, 2018).

systems have responded to recent breaches by adopting technology that helps make communication and transactions more secure, Defendants did not.

10. In addition to Defendants' failures to prevent the Data Breach, 24/7 also failed to disclose the Data Breach for approximately six (6) months, despite detecting and allegedly remedying the breach on October 12, 2017.[4]

11. The Data Breach was the inevitable result of Defendants' inadequate approach to data security and the protection of the Customer Data that it collected during the course of their business.

12. 24/7 acknowledges that it collects personal information, including: first and last names; organization names; email addresses; phone numbers; physical addresses; dates of birth; gender; professional title; account information; credit/debit card numbers; and other information 24/7 needs to provide client-specified services.[5] Indeed, 24/7 claims to follow "industry standards to protect the security of [users'] Personal Information and [24/7] respects [users'] choices for such information's intended use."[6] 24/7 allegedly uses "a combination of reasonable and appropriate physical, technical, and administrative safeguards to prevent unauthorized access or disclosure of [users'] Personal Information [… and] retains Personal Information and Interaction Data only as required or permitted by local law and while it has a legitimate business purpose."[7] Finally, 24/7 represents that it "uses standard security protocols, and mechanisms to exchange the transmission of sensitive Personal Information **such as credit card details and login credentials**."[8]

13. Best Buy has recognized that:

> Protecting customers' privacy is critical to Best Buy's growth and success. Customers entrust [Best Buy] with their personal information and it is [Best Buy's] responsibility to safeguard that data at all times. If Best Buy protects [its customers']

---

4 *Id.*

5 24/7, Inc., Platform Privacy Policy, *available at:* https://www.247.ai/privacy-policy#platform-policy (last visited April 30, 2018).

6 *Id.*

7 *Id.*

8 *Id.*

> personal information, customers are more likely to become, and remain, loyal to [Best Buy's] brand. If this trust is broken, Best Buy risks negative publicity, fines and lawsuits, lost sales, and damage to [Best Buy's] business and reputation."[9]

14. Delta acknowledges that "Information Security is important to Delta," and:

> [Delta has] established appropriate physical, electronic and managerial safeguards to protect the information we collect from or about our users. These safeguards are regularly reviewed to protect against unauthorized access, disclosure and improper use of your information, and to maintain the accuracy and integrity of that data.[10]

15. Delta further acknowledges that it collects: names, address, and telephone numbers; dates of birth; gender; redress numbers; known traveler numbers; email addresses; cell phone numbers; credit and debit card numbers, associated billing addresses, and expiration dates; emergency contacts, medical needs, and dietary requests; and other personal identifiable information.[11] Delta last updated this privacy policy on January 7, 2013.[12]

16. Delta further informs customers that it may engage third parties to process information and assist in improving the customer service experience, but "requires that these third parties comply with Delta's Privacy Policy" when processing customers' private and sensitive Customer Data.[13]

17. Unfortunately, Defendants, did not hold true to their security promises, despite any efforts to place the ultimate onus on consumers.

18. Instead, Defendants disregarded the rights of Plaintiffs and the Class and Subclass members, by, through themselves and their agent 24/7, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure Defendants' data systems were protected, failing to disclose to their customers the material

---

[9] Best Buy Code of Business Ethics, Privacy Policy, *available at:* https://secure.ethicspoint.com/domain/media/en/gui/26171/code.html?section=7&sub=4 (last visited April 30, 2018).

[10] Delta, Cookies, Privacy & Security, *available at:* https://www.delta.com/content/www/en_US/privacy-and-security.html (last visited April 30, 2018)

[11] *Id.*

[12] *Id.*

[13] *Id.*

fact that they did not have adequate computer systems and security practices to safeguard Customer Data, failing to take available steps to prevent and stop the breach from ever happening, failing to timely monitor and detect the Data Breach, and failing to timely notify consumers of the Data Breach.

19. In addition, 24/7, as the agent of Best Buy and Delta, exacerbated the damages Plaintiffs and the Class and Subclass members suffered by failing to timely detect the infiltration and failing to timely notify customers their Customer Data had been compromised. If 24/7 had detected the malware earlier and promptly notified Best Buy, Delta, and the public of the Data Breach, the resulting losses would have been far less significant.

20. As a result of Defendants' Data Breach, the Customer Data of Plaintiffs and the Class and Subclass members has been exposed to criminals for misuse, the obvious reason for which this information was taken . The damages Plaintiffs and the Class and Subclass members suffered as a direct result of the Data Breach include:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their debit or credit card accounts because their account were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Data Breach;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiffs' and the Class and Subclass members' information on the Internet black market;

h. money paid for merchandise purchased at Best Buy stores during the period of the Data Breach, in that Plaintiff and the Class and Subclass members would not have shopped at Best Buy had Defendants disclosed that they lacked adequate systems and procedures to reasonably safeguard customers' Customer Data, or Plaintiff and the Class and Subclass members would have taken measures to protect their Customer Data had Defendants made such disclosures;

i. damages to and diminution in value of their Customer Data entrusted to Defendants for the sole purpose of purchasing merchandise from Best Buy; and

j. the loss of Plaintiffs' and the Class and Subclass members' privacy.

21. The damages to Plaintiffs and the Class and Subclass members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for Customer Data.

22. The damages to Plaintiffs and the Class and Subclass members were also

directly and proximately caused by Defendants' failure to inform customers that their Customer Data was subject to collection and storage by the outsourced customer service corporation 24/7.

23. Further, Plaintiffs retain a significant interest in ensuring that their Customer Data, which, while stolen, remains in the possession of Defendants, is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and other similarly situated consumers whose Customer Data was stolen as a result of the Data Breach.

24. Plaintiffs, on behalf of themselves and other similarly situated consumers, seek to recover damages, equitable relief including injunctive relief to prevent a reoccurrence of the Data Breach and resulting injury, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendants.

26. This Court has personal jurisdiction over 24/7 because 24/7: 1) is headquartered in this District; 2) conducts substantial business in the District; and 3) committed the acts and omissions complained of in the District.

27. This Court has personal jurisdiction over Best Buy because Best Buy: 1) conducts substantial business in this District; and 2) committed the acts and omissions complained of in this District.

28. This Court has personal jurisdiction over Delta because Delta: 1) conducts substantial business in this District; and 2) committed the acts and omissions complained of in this District.

29. Venue is proper under 28 U.S.C. § 1391(c) because 24/7's principal places of business is in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including the decisions Defendants' management and IT personnel made that led to the Data Breach.

PARTIES

A. Plaintiff

30. Plaintiff Ford is a resident of the state of Texas.

31. Plaintiff Dubrovszky is a resident of the state of Oregon.

B. Defendant

32. 24/7 is a California corporation, which performs customer service functions for retailers and companies alike. 24/7's principal place of business and headquarters is located at 910 East Hamilton Avenue, Suite 240, Campbell, CA 95008, which is located in this District.

33. Best Buy is a Minnesota corporation, which owns and operates retail stores across the United States. Best Buy maintains its United States headquarters at 7601 Penn Avenue South, Richfield, Minnesota 55423.

34. Delta is a Delaware corporation, which provides air transportation for passengers in the United States and abroad. Delta maintains its United States headquarters at 1030 Delta Boulevard, Atlanta, Georgia 30354.

FACTUAL BACKGROUND

A. The Best Buy Plaintiff's Transactions

35. The Best Buy Plaintiff regularly makes purchases at Best Buy and uses the online chat function to communicate with customer service. For his purchases, he uses a credit card.

36. Recently, the Best Buy Plaintiff reviewed his financial statements and identified fraudulent activity in the amount of $370. Due to this fraudulent activity, he activated a fraud alert, froze his credit card account, and requested a new one.

37. The compromise of the Best Buy Plaintiff's payment card occurred even though he had physical possession of the card at all times. He was required to expend time communicating with the card issuer attempting to resolve the issues caused by the theft of his credit card and other personal information used to accomplish the fraudulent activity.

38. The Best Buy Plaintiff would not have used his payment card, Best Buy's online store, and Best Buy's agent 24/7's customer service client to make purchases at and communicate with Best Buy had 24/7 and Best Buy told him they lacked adequate computer systems and data security practices to safeguard customers' Customer Data from theft. Indeed, the Best Buy Plaintiff would not have shopped at Best Buy at all during the period of the Data Breach and, thus, he suffered actual injury and damages in paying money for the purchase of merchandise from Best Buy that he would not have paid had 24/7 and Best Buy made such disclosures.

39. The Best Buy Plaintiff suffered actual injury from having his Customer Data compromised and stolen in and as a result of the Data Breach.

40. The Best Buy Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his Customer Data—a form of intangible property that he entrusted to Best Buy and its agent 24/7 as a form of payment for merchandise and that was compromised in and as a result of the Data Breach.

41. The Best Buy Plaintiff further suffered actual injury in the form of time spent dealing with fraud resulting from the Data Breach, disputing the fraudulent charges, and monitoring his account for additional fraud.

42. Additionally, the Best Buy Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Customer Data being placed in the hands of criminals who have already misused such information, as evidenced by the compromise of his payment card.

43. Moreover, the Best Buy Plaintiff has a continuing interest in ensuring that his private information, which remains in the possession of 24/7 and Best Buy, is protected and safeguarded from future breaches.

B. The Delta Plaintiff's Transactions

44. The Delta Plaintiff makes purchases with Delta through Delta's mobile application and website, and uses the online chat function to communicate with customer service. For his purchases, he uses a credit card.

45. Recently, the Delta Plaintiff reviewed his financial statements and identified numerous transactions that were determined to be fraudulent activity. Due to this fraudulent activity, he changed his passwords and signed up for fraud protection services.

46. The compromise of the Delta Plaintiff's payment card occurred even though he had physical possession of the card at all times. He was required to expend time communicating with the card issuer attempting to resolve the issues caused by the theft of his credit card and other personal information used to accomplish the fraudulent activity.

47. The Delta Plaintiff would not have used his payment card, Delta's website and mobile app, and Delta's agent 24/7's customer service client to make Delta purchases and communicate with Delta had 24/7 and Delta told him they lacked adequate computer systems and data security practices to safeguard customers' Customer Data from theft. Indeed, the Delta Plaintiff would not have patronized Delta at all during the period of the Data Breach and, thus, he suffered actual injury and damages in paying money for the purchase of air travel from Delta that he would not have paid had 24/7 and Delta made such disclosures.

48. The Delta Plaintiff suffered actual injury from having his Customer Data compromised and stolen in and as a result of the Data Breach.

49. The Delta Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his Customer Data—a form of intangible property that he entrusted to Delta and its agent 24/7 as a form of payment for merchandise and that was compromised in and as a result of the Data Breach.

50. The Delta Plaintiff further suffered actual injury in the form of time spent dealing with fraud resulting from the Data Breach, disputing the fraudulent charges, signing up for third-party monitoring, and monitoring his account for additional fraud.

51. Additionally, the Delta Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Customer Data being placed in the hands of criminals who have already misused such information, as evidenced by the compromise of his payment card.

52. Moreover, the Delta Plaintiff has a continuing interest in ensuring that his private information, which remains in the possession of 24/7 and Delta, is protected and safeguarded from future breaches.

C. Defendants Collect and Store PII for their Own Financial Gain

53. Founded in 2000,[14] 24/7 operates a variety of customer services products with artificial intelligence technologies with additional offices in Toronto, London, Stockholm, and Sydney, and numerous clients in retail, education, financial services, healthcare, insurance, travel and hospitality, and utilities.[15]

54. Since its founding, 24/7 has aggressively expanded, including private funding from Sequoia Capital—a venture capital firm controlling $1.4 trillion in assets—in 2003, as well as a partnership with Microsoft in 2012, in which Microsoft combined its "interactive self-service assets" with 24/7's technologies.[16]

55. At all relevant times, Defendants were well-aware, or reasonably should have been aware, that the Customer Data collected, maintained, and stored in their agent 24/7's computer systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

56. It is well known and the subject of many media reports that Customer Data is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches by other retailers, Defendants maintained an insufficient and inadequate system to protect Plaintiff's and the Class and Subclass members'

---

[14] [24]7 Company Profile, Forbes, https://www.forbes.com/companies/24-7/ (last visited April 30, 2018);

[15] [24]7 Company Overview, https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=4532786 (last visited April 30, 2018)

[16] *Microsoft picks stake in Sequoia-backed 24/7 Inc*, Reuters, https://in.reuters.com/article/microsoft-picks-stake-in-sequoia-backed-idINDEE81807U20120209 (last visited May 1, 2018)

Customer Data.

57. Customer Data is a valuable commodity because it contains not only payment card numbers but PII as well. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers, and other personal information on a number of underground Internet websites. Customer Data is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

58. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[17]

59. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Customer Data and of the foreseeable consequences that would occur if Defendants', and particular 24/7's (as an agent of each Defendant), data security systems were breached, including, specifically, the significant costs that would be imposed on their customers as a result of a data breach.

60. Defendants were, or reasonably should have been, fully aware of the significant volume of daily credit and debit card transactions and PII provided in customer service interactions and purchase and, thus, the significant number of individuals who would be harmed by a breach of Defendants' systems.

61. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of Customer Data in the hands of other third parties, such as retailers, Defendants' approach to maintaining the privacy and security

[17] Verizon 2014 PCI Compliance Report, available at: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited April 30, 2018).

Plaintiffs' and the Class and Subclass members' Customer Data was lackadaisical, cavalier, reckless, or at the very least, negligent.

D. Defendants Had Notice of Data Breaches Involving Malware on POS Systems

62. A wave of data breaches causing the theft of retail payment card information has hit the United States in the last several years.[18] In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year.[19] The amount of payment card data compromised by data breaches is massive. For example, it is estimated that over 100 million cards were compromised in 2013 and 2014.[20]

63. Most of the massive data breaches occurring within the last several years involved malware placed on computer systems that retail merchants and their agents use.

64. These massive data breaches involve compromising payment systems at physical retail outlets, phishing schemes to gain access to internal servers and information, as well as exploiting other vulnerabilities in companies' websites and electronically stored data systems.

E. Defendants' Data Breach

65. On April 4, 2018, Delta announced the Data Breach, and on April 5, 2018, Best Buy followed. According to their respective statements, Best Buy and Delta were informed of the Data Breach on March 28, 2018.

66. 24/7 possibly knew of the Data Breach as early as September 26, 2017, and definitively on October 12, 2017, when 24/7 allegedly fixed the security issues.[21]

---

[18] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, Identity Theft Resource Center (Jan. 19, 2017), http://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208 (last visited April 13, 2018).

[19] *Id.*

[20] Symantec, *A Special Report On Attacks On Point-of-Sale Systems*, p. 3 (Nov. 20, 2014), available at: https://origin-www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf (last visited April 13, 2018).

[21]

67. Despite knowing of the Data Breach as of October 12, 2017—over six (6) months ago—24/7 has not provided much-if-any details regarding the degree and extent of the Data Breach, despite handling chat services for Best Buy, Delta, Sears, and a number of other companies.

F. The Data Breach Caused Harm and Will Result in Additional Fraud

68. Without detailed disclosure of the nature and scope of the Data Breach, consumers, including Plaintiffs and the Class and Subclass members, have been left exposed—unknowingly and unwittingly—for months to continued misuse and ongoing risk of misuse of their personal information without being able to take necessary precautions to prevent imminent harm.

69. The ramifications of Defendants' failure to keep Plaintiffs' and the Class and Subclass members' Costumer Data secure are severe.

70. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[22] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[23]

71. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[24]

72. Identity thieves can use personal information, such as Plaintiffs' and the Class and Subclass members', which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's

[22] 17 C.F.R § 248.201 (2013).

[23] *Id.*

[24] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 13, 2018).

information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

73. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[25]

74. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[26]

75. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[27]

76. Plaintiffs and the Class and Subclass members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and the Class and Subclass members are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them

---

[25] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited April 13, 2018).

[26] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 13, 2018).

[27] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited April 13, 2018).

and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

G. Plaintiffs and the Class and Subclass Members Suffered Damages

77. Plaintiffs' and the Class and Subclass members' Customer Data is private and sensitive in nature, and Defendants left that Customer Data inadequately protected. Defendants did not obtain Plaintiffs' and the Class and Subclass members' consent to disclose their Customer Data to any other person as required by applicable law and industry standards.

78. The Data Breach was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiffs' and the Class and Subclass members' Customer Data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and the Class and Subclass members' Customer Data to protect against reasonably foreseeable threats to the security or integrity of such information.

79. Defendants had the resources to prevent a breach, especially with the partnerships with Sequoia Capital and Microsoft.

80. Had Defendants employed security measures recommended by experts in the field, Defendants would have prevented intrusion into their computer systems and, ultimately, the theft of their customers' Customer Data.

81. As a direct and proximate result of Defendants' wrongful actions and inaction and the resulting Data Breach, Plaintiffs and the Class and Subclass members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions,

closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a retailer's slippage, as is the case here.

82. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and the Class and Subclass members' Customer Data, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiffs' and the Class and Subclass members' information on the Internet black market;

d. the untimely and inadequate notification of the Data Breach;

e. the improper disclosure of their Customer Data;

f. loss of privacy;

g. the monetary amount of purchases at Best Buy and Delta during the period of the Data Breach in that Plaintiffs and the Class and Subclass members would not have patronized Best Buy and Delta, or at least would not have used their payment cards for online purchases, had Defendants disclosed that Defendants lacked adequate systems and procedures to reasonably safeguard customers' financial and personal

information and had Defendants provided timely and accurate notice of the Data Breach;

h. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

i. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

j. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

k. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

l. the loss of productivity and value of their time spent to address attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

83. Best Buy and Delta—but not 24/7—have stated that affected customers will be offered credit monitoring or identity theft protection services, but have not come forth with any details as to how to sign up, the type of coverage, the scope of coverage, or the length of coverage. As a result, Plaintiffs and the Class and Subclass members are left to their own actions to protect

themselves from the financial damage Defendants have allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Defendants' actions have created for Plaintiffs and the Class and Subclass members is ascertainable and is a determination appropriate for the trier of fact.

84. While Plaintiffs' and the Class and Subclass members' Customer Data has been stolen, Defendants continue to hold Customer Data of consumers, including Plaintiffs, the Class members, and the subclass members. Particularly because Defendants have demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and the Class and Subclass members have an undeniable interest in ensuring that their Customer Data is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CHOICE OF LAW

85. California, which seeks to protect the rights and interests of California and other U.S. residents against a company doing business in California, has a greater interest in the claims of Plaintiffs and the Class and Subclass members than any other state and is most intimately concerned with the claims and outcome of this litigation.

86. The principal place of business of 24/7—which both Best Buy and Delta entrusted to provide services as their agent—is located at 910 East Hamilton Avenue, Suite 240, Campbell, CA 95008, is the "nerve center" of 24/7's business activities—the place where high-level officers direct, control, and coordinate 24/7's activities, including data security, and where: a) major policy; b) advertising; c) distribution; d) accounts receivable departments; and e) financial and legal decisions originate.

87. Data security assessments and other IT duties related to computer systems and data security occur at 24/7's California headquarters.

88. Furthermore, 24/7's response, and corporate decisions surrounding such response, to the Data Breach were made from and in California.

89. 24/7's breach of their duty to customers—including Plaintiff and the Class and Subclass members—emanated from California.

90. Moreover, because 24/7 is headquartered in California and its key decisions and operations emanate from California, California law can and should apply to claims relating to the Data Breach, even those made by persons who reside outside of California. In fact, California law should apply to all of Plaintiffs' claims, as Best Buy and Delta entrusted 24/7 to handle and make decisions, and 24/7**'s** substandard acts happened in California, and, upon information and belief, the Plaintiff's PII was collected, stored on, and routed through California-, and United States-based servers. For the sake of fairness and efficiency, California law should apply to these claims.

91. Application of California law to a nationwide Class with respect to Plaintiffs' and the Class and Subclass members' claims is neither arbitrary nor fundamentally unfair because California has significant contacts and a significant aggregation of contacts that create a state interest in the claims of the Plaintiffs, the nationwide Class, and the respective subclasses.

92. Further, under California's choice of law principles, which are applicable to this action, the common law of California will apply to the common law claims of all Class members.

CLASS ACTION ALLEGATIONS

93. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure, Plaintiffs bring this lawsuit on behalf of themselves and as a class action on behalf of the following classes of individuals:

NATIONWIDE CLASS: (or the CLASS)	All persons who used 24/7's electronic customer service platform and whose Customer Data was compromised as a result of the Data Breach.
BEST BUY SUBCLASS:	All consumers who used Best Buy's electronic customer service platform and whose Customer Data was compromised as a result of the Data Breach.
DELTA SUBCLASS:	All consumers who used Delta's electronic

customer service platform and whose Customer Data was compromised as a result of the Data Breach.

94. Excluded from the Class are Defendants and any entities in which any Defendant or their subsidiaries or affiliates have a controlling interest; Defendants' officers, agents, and employees; and all persons who make a timely election to be excluded from the Nationwide Class and any subclasses. Also excluded from the Class are the judge assigned to this action, and any member of the judge's immediate family.

95. **Numerosity:** The members of each Class are so numerous that joinder of all members of any Class would be impracticable. Plaintiffs reasonably believe that the Nationwide Class members number in the hundreds of thousands of people or more in the aggregate, and well over 1,000 in the smallest of the classes. Similarly, Plaintiffs reasonably believe that the Best Buy and Delta Subclass members number in the hundreds of thousands of people or more in the aggregate, and well over 1,000 in the smallest of classes. The names and addresses of the Class and Subclass members are identifiable through documents Defendants maintain.

96. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual Class and Subclass members, including:

i. Whether Defendants owed a legal duty to Plaintiffs and the Class and Subclass members to exercise due care in collecting, storing, and safeguarding their Customer Data;

ii. Whether Defendants breached a legal duty to Plaintiffs and the Class and Subclass members to exercise due care in collecting, storing, and safeguarding their Customer Data;

iii. Whether Defendants knew or should have known of the susceptibility of their computer systems to a data breach;

iv. Whether Defendants' security measures to protect their computer systems were reasonable in light of industry data security

recommendations, and other measures data security experts recommended;

v. Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the Class and Subclass members' Customer Data;

vi. Whether Plaintiffs' and the Class and Subclass members' Customer Data was accessed, exposed, compromised, or stolen in the Data Breach;

vii. Whether Defendants were negligent in failing to implement reasonable and adequate security procedures and practices;

viii. Whether Defendants' failure to implement adequate data security measures allowed the breach of their computer systems to occur;

ix. Whether Defendants' conduct constituted deceptive trade practices under California law;

x. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in the loss of Plaintiffs' and the Class and Subclass members' Customer Data;

xi. Whether Defendants failed to timely notify the public of the Data Breach;

xii. Whether Defendants' conduct violated Cal. Civ. Code § 1750, *et seq.*;

xiii. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

xiv. Whether Defendants' conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq.*;

xv. Whether Plaintiffs and the Class and Subclass members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

xvi. Whether Plaintiffs and the Class and Subclass members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

97. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the Class and Subclass members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

98. **Typicality:** Plaintiffs' claims are typical of the Class and Subclass members' claims because, among other things, Plaintiffs and the Class and Subclass members were injured through Defendants' substantially uniform misconduct. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and the Class and Subclass members, and there are no defenses that are unique to Plaintiffs' claims. Plaintiffs' and the Class and Subclass members' claims arise from the same operative facts and are based on the same legal theories.

99. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Nationwide Class and the respective subclasses because their interests do not conflict with the interests of the other class and subclass members they seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation; and Plaintiffs will prosecute this action vigorously. The Class and subclass members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

100. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the Class and Subclass members are relatively small compared to the burden and expense that would be required

to litigate their claims on an individual basis against Defendants, making it impracticable for the Class and Subclass members to individually seek redress for Defendants' wrongful conduct. Even if the Class and Subclass members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

101. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and Subclass and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

102. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether the Class and Subclass members' Customer Data was accessed, exposed, compromised, or stolen in the Data Breach;

b. Whether (and when) Defendants knew about the Data Breach before it was announced to the public and whether Defendants failed to timely notify the public of the Data Breach;

c. Whether Defendants misrepresented the safety of their many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs and the Class and Subclass members' Customer Data;

d. Whether Defendants concealed crucial information about their inadequate data security measures from Plaintiffs and the Class and Subclass members;

e. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendants' acts, omissions, misrepresentations, and practices were and are likely to deceive consumers;

g. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and the Class and Subclass members' Customer Data secure and prevent the loss or misuse of that information;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices for Plaintiffs' and the Class and Subclass members' Customer Data in violation of Section 5 of the FTC Act;

i. Whether Defendants failed to provide timely notice of the Data Breach, to Plaintiff and the Class and Subclass members;

j. Whether Defendants conduct violated Cal. Bus. & Prof. Code § 22575, *et seq.*;

k. Whether Defendants owed a duty to Plaintiffs and the Class and Subclass members to safeguard their Customer Data and to implement adequate data security measures;

l. Whether Defendants failed to adhere to their posted privacy policies concerning the care they would take to safeguard Plaintiffs' and the Class and Subclass members' Customer Data in violation of Cal. Bus. & Prof. Code § 22576;

m. Whether Defendants negligently and materially failed to adhere to their posted privacy policies concerning the safeguarding of Plaintiffs' and the Class and Subclass members' Customer Data in violation of Cal. Bus. & Prof. Code § 22576;

n. Whether Defendants breached that duty;

o. Whether an implied contract existed between Defendants and Plaintiffs and the Class and Subclass members, and the terms of any such implied contract; and,

p. Whether Defendants breached the implied contract.

CLAIMS ALLEGED ON BEHALF OF THE CLASS

First Claim for Relief
Violation of California's Unfair Competition Law ("UCL")
Unlawful Business Practice
(Cal. Bus. & Prof. Code § 17200, *et seq.*)
(On Behalf of Plaintiffs, the Nationwide Class, the Best Buy Subclass, and the Delta Subclass)

103. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 102 as though fully stated herein.

104. By reason of the conduct alleged herein, Defendants engaged in unlawful "business practices" within the meaning of the UCL.

105. Since at least September 2017, 24/7 has been the customer support provider and agent of Best Buy and Delta to provide customer service support to their respective customers. 24/7 is the agent of both Best Buy and Delta.

106. 24/7 stored the Customer Data of Plaintiffs and the Class and Subclass members on behalf of Best Buy and Delta in its computer systems. Defendants falsely represented to Plaintiffs and the Class and Subclass members that their Customer Data was secure and would remain private.

107. Defendants knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiffs' and the Class and Subclass members' Customer Data secure and prevented the loss or misuse of that Customer Data.

108. Even without these misrepresentations, Plaintiffs and the Class and Subclass members were entitled to assume, and did assume Defendants would take appropriate measures to keep their Customer Data safe. Defendants did not disclose at any time that Plaintiffs' Customer Data was vulnerable to hackers because Defendants' data security measures were inadequate and outdated, and Defendants were the only ones in possession of that material information, which they had a duty to disclose. Defendants violated the UCL by misrepresenting, both by affirmative conduct and by omission, the safety of their computer systems, specifically the security thereof, and their ability to safely store Plaintiffs' and the Class and Subclass members' Customer Data. Defendants also violated the UCL by failing to implement reasonable and appropriate security measures or follow industry standards for data security, failing to comply with their own posted privacy policies, and by failing to immediately notify Plaintiffs and the Class and Subclass members of the Data Breach. If Defendants had complied with these legal requirements, Plaintiffs and the Class and Subclass members would not have suffered the damages related to the Data Breach, and consequently from, Defendants' failure to timely notify Plaintiffs and the Class and Subclass members of the Data Breach.

109. Defendants' acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the Federal Trade Commission Act.

110. Plaintiffs and the Class and Subclass members suffered injury in fact and lost money or property as the result of Defendants' unlawful business practices. In particular, Plaintiffs and the Class and Subclass members have suffered from improper or fraudulent charges to their credit/debit card accounts; and other similar harm, all as a result of the Data Breach. In addition, their Customer Data was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the

hacked information is of tangible value. Plaintiffs and the Class and Subclass members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

111. As a result of Defendants' unlawful business practices, violations of the UCL, Plaintiffs and the Class and Subclass members are entitled to injunctive relief.

Second Claim for Relief
Violation of California's Unfair Competition Law ("UCL")
Unfair Business Practice
(Cal. Bus. & Prof. Code § 17200, *et seq.*)
(On Behalf of Plaintiffs, the Nationwide Class, the Best Buy Subclass, and the Delta Subclass)

112. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 102 as though fully stated herein.

113. By reason of the conduct alleged herein, Defendants engaged in unfair "business practices" within the meaning of the UCL.

114. Defendants stored Plaintiffs' and the Class and Subclass members' Customer Data in their electronic and consumer information databases. Defendants represented to Plaintiffs and the Class and Subclass members that their Customer Data databases were secure and that Plaintiffs' and the Class and Subclass members' Customer Data would remain private. Best Buy and Delta, themselves and through their agent 24/7, engaged in unfair acts and business practices by representing that they had secure computer systems when they did not.

115. Even without these misrepresentations, Plaintiffs and the Class and Subclass members were entitled to, and did, assume Defendants would take appropriate measures to keep their Customer Data safe. Defendants did not disclose at any time that Plaintiffs' Customer Data was vulnerable to hackers because Defendants' data security measures were

inadequate and outdated, and Defendants were the only ones in possession of that material information, which they had a duty to disclose.

116. Defendants knew or should have known they did not employ reasonable measures that would have kept Plaintiffs' and the Class and Subclass members' Customer Data secure and prevented the loss or misuse of Plaintiffs' and the Class and Subclass members' Customer Data.

117. Defendants violated the UCL by misrepresenting, both by affirmative conduct and by omission, the security of their systems and services, and their ability to safely store Plaintiffs' and the Class and Subclass members' Customer Data. Defendants also violated the UCL by failing to implement and maintain reasonable security procedures and practices appropriate to protect Customer Data, and by failing to immediately notify Plaintiffs and the Class and Subclass members of the Data Breach.

118. Defendants also violated their commitment to maintain the confidentiality and security of Plaintiffs' and the Class and Subclass members' Customer Data, and failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security.

119. **Defendants engaged in unfair business practices under the "balancing test."** The harm caused by Defendants' actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendants' failure to follow basic data security protocols and misrepresentations to consumers about Defendants' data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiffs and the Class and Subclass members, directly causing the harms alleged below.

120. **Defendants engaged in unfair business practices under the "tethering test."** Defendants' actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.,* Cal. Civ. Code § 1798.1 ("The Legislature declares that ... all individuals have a right of privacy in information pertaining to them.... The increasing use of computers ... has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.") Defendants' acts and omissions, and the injuries caused by them, are thus "comparable to or the same as a violation of the law …" *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal.4th 163, 187.

121. **Defendants engaged in unfair business practices under the "FTC test."** The harm caused by Defendants' actions and omissions, as described in detail above, is substantial in that it affects hundreds of thousands of Class and Subclass members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiffs' and the Class and Subclass members' Customer Data to third parties without their consent, diminution in value of their Customer Data, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiffs' and the Class and Subclass members' Customer Data remains in Defendants' possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendants' actions

and omissions violated, *inter alia*, Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.,* 10 F. Supp. 3d 602, 613 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act); *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (same); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil Action No. 1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) ("failure to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security. confidentiality, and integrity of personal information collected from or about consumers" violates § 5(a) of FTC Act); 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

122. Plaintiffs and the Class and Subclass members suffered injury in fact and lost money or property as the result of Defendants' unfair business practices. In particular, Plaintiffs and the Class and Subclass members have suffered from improper or fraudulent charges to their credit/debit card accounts; and other similar harm, all as a result of the Data Breach. In addition, their Customer Data was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and the Class and Subclass members have also suffered consequential out of pocket losses for procuring credit freeze or protection

services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

123. As a result of Defendants' unfair business practices, violations of the UCL, Plaintiffs and the Class and Subclass members are entitled to injunctive relief.

Third Claim for Relief
Negligence
(On Behalf of Plaintiffs, the Nationwide Class, the Best Buy Subclass, and the Delta Subclass)

124. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 102 as though fully stated herein.

125. Upon accepting and storing Plaintiffs' and the Class and Subclass members' Customer Data in their computer systems and on their networks, Defendants undertook and owed a duty to Plaintiffs and the Class and Subclass members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the Customer Data was private and confidential, and should be protected as private and confidential. 24/7 owed this duty to the Nationwide Class, as well as the Best Buy and Delta Subclasses; Best Buy owed this duty to the Best Buy Subclass; and Delta owed this duty to the Delta Subclass.

126. Defendants owed these respective duties of care not to subject Plaintiffs and the Class and Subclass members, along with their Customer Data, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

127. Defendants owed a duty to Plaintiffs and the Class and Subclass members to exercise reasonable care in safeguarding and protecting their Customer Data and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendants' security systems to ensure Plaintiffs' and the Class and Subclass members' Customer Data was adequately secured and protected. Defendants further had a duty to implement processes that would detect a breach of their data system in a timely manner. 24/7 owed

these duties to the Nationwide Class, as well as the Best Buy and Delta Subclasses; Best Buy owed these duties to the Best Buy Subclass; and Delta owed these duties to the Delta Subclass.

128. Defendants knew that Plaintiffs' and the Class and Subclass members' Customer Data was personal and sensitive information that is valuable to identity thieves and other criminals. Defendants also knew of the serious harms that could happen if Plaintiffs' and the Class and Subclass members' Customer Data was wrongfully disclosed, that disclosure was not fixed, or Plaintiffs and the Class and Subclass members were not told about the disclosure in a timely manner.

129. By being entrusted by Plaintiffs and the Class and Subclass members to safeguard their respective Customer Data, Defendants had special relationships with Plaintiffs and the Class and Subclass members; Plaintiffs and the Class and Subclass members utilized 24/7 product, and patronized Best Buy and Delta, and accepted Best Buy's and Delta's respective offers to use payment cards as an approved form of payment through 24/7's customer support platform. Plaintiffs and the Class and Subclass members did so with the understanding that Defendants would take appropriate measures to protect their respective Customer Data and would inform Plaintiffs and the Class and Subclass members of any breaches or other security concerns that might call for action. But, Defendants did not. Defendants not only knew their data security was inadequate, they also knew they didn't have the tools to detect and document intrusions or exfiltration of Customer Data. Defendants are morally culpable, given their wholly inadequate safeguards, as well as their refusal to notify Plaintiffs and the Class and Subclass members of breaches or security vulnerabilities.

130. Defendants breached their respective duties to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class and Subclass members' Customer Data by failing to adopt, implement, and maintain adequate security measures to safeguard that information, and allowing unauthorized access to Plaintiffs' and the Class and Subclass members' Customer Data.

131. Defendants also breached their respective duties to timely disclose that Plaintiffs' and the Class and Subclass members' Customer Data had been, or was reasonably believed to have been, stolen, exposed, or compromised.

132. Defendants' failure to comply with industry further evidences Defendants' negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class and Subclass members' Customer Data.

133. But for Defendants' respective wrongful and negligent breach of their respective duties owed to Plaintiffs and the Class and Subclass members, their Customer Data would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' respective negligence was a direct and legal cause of the theft of Plaintiffs' and the Class and Subclass members' Customer Data, as well as the resulting damages.

134. The injury and harm Plaintiffs and the Class and Subclass members suffered was the reasonably foreseeable result of Defendants' respective failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class and Subclass members' Customer Data. Defendants knew their computer systems and technologies for accepting and securing Plaintiffs' and the Class and Subclass members' Customer Data had numerous security vulnerabilities.

135. Defendants' respective misconduct as alleged herein was willful and with conscious disregard of Plaintiffs' and the Class and Subclass members' rights or safety, and despicable conduct that has subjected Plaintiffs and the Class and Subclass members to cruel and unjust hardship in conscious disregard of their rights.

136. As a result of Defendants' respective misconduct, Plaintiffs' and the Class and Subclass members' Customer Data was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their Customer Data was disclosed to third parties without their consent. Plaintiff and the Class and Subclass members also suffered diminution in value of their Customer Data in that it is now easily available to hackers on the dark web. Plaintiffs and the Class and Subclass members have also suffered consequential out of pocket losses for procuring credit freeze or protection services,

identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Fourth Claim for Relief
Breach of Implied Contract
(On Behalf of Plaintiffs, the Best Buy Subclass, and the Delta Subclass)

137. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 102 as though fully stated herein.

138. Best Buy solicited and invited the Best Buy Plaintiff and the Best Buy Subclass members to use the electronic customer support platform to make purchases using their credit or debit cards. The Best Buy Plaintiff and the Best Buy Subclass members accepted Best Buy's offer and used their credit or debit cards to patronize Best Buy during the period of the Data Breach.

139. Delta solicited and invited the Delta Plaintiff and the Delta Subclass members to use the electronic customer support platform to make purchases using their credit or debit cards. The Delta Plaintiff and the Delta Subclass members accepted Delta's offer and used their credit or debit cards to patronize Delta during the period of the Data Breach.

140. When Plaintiffs and the Subclass members respectively patronized Best Buy and Delta using payment cards, they provided their Customer Data, including but not limited to the PII of their debit and credit cards. In so doing, Plaintiffs and the Subclass members entered into implied contracts with Best Buy and Delta, respectively, pursuant to which Best Buy and Delta, respectively, agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and the Subclass members if their data had been breached and compromised.

141. Each purchase Plaintiffs and the Subclass members made at Best Buy or Delta, respectively, using their credit or debit card was made pursuant to the mutually agreed-upon implied contract with that Defendant, under which that Defendant agreed to safeguard and protect the Customer Data of Plaintiffs and the Subclass members, including

Plaintiffs' and the Subclass members' PII and credit or debit cards, and to timely and accurately notify them if such information was compromised or stolen.

142. Plaintiffs and the Subclass members would not have provided and entrusted their Customer Data, including PII and credit and debit card information, to the respective Defendant to make purchases in the absence of the implied contract between them and the respective Defendant.

143. Plaintiffs and the Subclass members fully performed their obligations under the respective implied contracts with Defendants.

144. Defendants breached the respective implied contracts made with Plaintiffs and the Subclass members by failing to safeguard and protect Plaintiffs' and the Subclass members' Customer Data by failing to provide timely and accurate notice to them that their Customer Data was compromised as a result of the Data Breach.

145. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiffs and the Subclass members sustained actual losses and damages, including nominal damages, as described in detail above. These breaches of implied contracts were a direct and legal cause of the injuries and damages to Plaintiffs and the Subclass members, as described above.

Fifth Claim for Relief
Negligence Per Se
(On Behalf of Plaintiffs, the Nationwide Class, the Best Buy Subclass, and the Delta Subclass)

146. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 102 as though fully stated herein.

147. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Customer Data.

148. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Customer Data and not complying with applicable industry standards.

Defendants' conduct was particularly unreasonable given the nature and amount of Customer Data they obtained and stored, and the foreseeable consequences of a data breach at Best Buy and Delta, including, specifically, the immense damages that would result to Plaintiffs and the Class and Subclass members.

149. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

150. Plaintiffs and the Class and Subclass members are within the class of persons the FTC Act was intended to protect.

151. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that Plaintiffs and the Class and Subclass members suffered.

152. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class and Subclass members have suffered, and continue to suffer, injuries and damages arising from Plaintiffs' and the Class and Subclass members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

Sixth Claim for Relief
Unjust Enrichment
(On Behalf of Plaintiffs, the Nationwide Class, the Best Buy Subclass, and the Delta Subclass)

153. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 102 as though fully stated herein.

154. Plaintiffs and the Class and Subclass members conferred a monetary benefit on Defendants. Specifically, the Best Buy Plaintiff and the Best Buy Subclass patronized and provided Best Buy with their payment information through Best Buy's agent 24/7. In exchange, the Best Buy Plaintiff and the Best Buy Subclass members should have received from Best Buy the goods and services that were the subject of the transaction and should have been entitled to have Best Buy and its agent 24/7 protect their Customer Data with adequate data security.

155. Also, the Delta Plaintiff and the Delta Subclass members patronized and provided Delta with their payment information through Delta's agent 24/7. In exchange, the Delta Plaintiff and the Delta Subclass members should have received from Delta the goods and services that were the subject of the transaction and should have been entitled to have Delta and its agent 24/7 protect their Customer Data with adequate data security.

156. Further, the Plaintiffs and the Class members provided 24/7 with their payment information and Customer Data, to be provided to 24/7's principals. In exchange, the Plaintiffs and the Class members should have received from 24/7's principals the goods and services that were the subject of the transaction and should have been entitled to have those principals and their agent 24/7 protect their Customer Data with adequate data security.

157. Defendants knew that the respective Plaintiffs and the Class and Subclass members conferred those benefits on the respective Defendant, and the respective Defendant accepted or retained that benefit. Defendants profited from the purchases and used Plaintiffs' and the Class and Subclass members' Customer Data for business purposes.

158. Defendants failed to secure Plaintiffs' and the Class and Subclass members' Customer Data and, therefore, did not provide full compensation for the benefit Plaintiffs and the Class and Subclass members provided.

159. Defendants acquired the Customer Data through inequitable means and failed to disclose the inadequate security practices previously alleged.

160. If Plaintiffs and the Class and Subclass members knew that Defendants would not secure their Customer Data using adequate security, they would not have patronized the respective Defendants and other principals that contracted with 24/7 to collect and transmit the Customer Data.

161. Plaintiffs and the Class and Subclass members have no adequate remedy at law.

162. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and the Class and Subclass members conferred.

163. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and the Class and Subclass members, proceeds that Defendants unjustly received from Plaintiff and the Class and Subclass members. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and the Class and Subclass members overpaid.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class and Subclass members, respectfully request that this Court enter an Order:

a. Certifying the Nationwide Class, the Best Buy Subclass, and the Delta Subclass, and appointing Plaintiffs and their Counsel to represent the Nationwide Class, the Best Buy Subclass, and the Delta Subclass;

b. Finding that Defendants' conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

c. Enjoining Defendants from engaging in further negligent, deceptive, unfair, and unlawful business practices alleged herein;

d. Awarding Plaintiffs and the Class and Subclass members actual, compensatory, consequential, and/or nominal damages;

e. Awarding Plaintiffs and the Class and Subclass members statutory damages and penalties, as allowed by law;

f. Requiring Defendants to provide appropriate credit monitoring services to Plaintiffs and the Class and Subclass members;

g. Compelling Defendants to use appropriate cyber security methods and policies with respect to data collection, storage, and protection, and to disclose with specificity to the Class and Subclass members the type of Customer Data compromised;

h. Awarding Plaintiffs and the Class and Subclass members pre-judgment and post-judgment interest;

i. Awarding Plaintiffs and the Class and Subclass members reasonable attorneys' fees, costs and expenses, and;

j. Granting such other relief as the Court deems just and proper.

Dated: May 10th, 2018

/s/ Joshua H. Watson

CLAYEO C. ARNOLD
California SBN 65070
carnold@justice4you.com
JOSHUA H. WATSON
California SBN 238058
Email: jwatson@justice4you.com
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, California 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

JOHN A. YANCHUNIS*
jyanchunis@ForThePeople.com
RYAN J. MCGEE*
rmcgee@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

Attorneys for Plaintiff and the Proposed Class

* *pro hac vice* application to be submitted